CUAUHTEMOC ORTEGA (Bar No. 257443)
Federal Public Defender
TERRA CASTILLO LAUGHTON (Bar No. 321683)
(E-Mail: terra_laughton@fd.org)
Deputy Federal Public Defender
411 West Fourth Street, Suite 7110
Santa Ana, California 92701-4598
Telephone: (714) 338-4500
Facsimile: (714) 338-4520

Attorneys for Defendant
RENE RODRIGUEZ

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. RENE RODRIGUEZ. Defendant.	Case No. 8:23-cr-00123-DOC **DEFENDANT'S MOTION TO SUPPRESS EVIDENCE OBTAINED IN VIOLATION OF THE FOURTH AMENDMENT; EXHIBITS** Hearing Date: 7/22/24 at 1:30 p.m. Trial Date: 8/6/24 Status Conference: None

PLEASE TAKE NOTICE that on July 22, 2024 at 1:30 p.m., or as soon thereafter as counsel may be heard in the courtroom of the Honorable David O. Carter, United States District Judge, Defendant Rene Rodriguez, by and through his attorney of record Deputy Federal Public Defender Terra Castillo Laughton, will and does hereby move this Court for an order suppressing all evidence law enforcement obtained in violation of his Fourth Amendment rights.

MOTION

This Motion is made pursuant to the Fourth Amendment of the United States Constitution, and such other statutory and constitutional rules as may be applicable, and is based upon the attached memorandum of points and authorities; the accompanying declaration and exhibits, including the declaration of Mr. Rodriguez; the files and records in this case; and any evidence and argument presented at a hearing on this motion.

Mr. Rodriguez specifically requests an evidentiary hearing.

The parties conferred regarding this Motion on multiple occasions, including April 12, 2024, May 16, 2024, and June 20, 2024.

Respectfully submitted,

CUAUHTEMOC ORTEGA
Federal Public Defender

DATED: June 24, 2024

By */s/ Terra D. Castillo Laughton*
Terra Castillo Laughton
Deputy Federal Public Defender
Attorney for Rene Rodriguez

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

TABLE OF AUTHORITIES

Page(s)

TABLE OF AUTHORITIES

Page(s)

Other Authorities

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Over the course of its five-year investigation in this case, the government repeatedly flouted court orders and Mr. Rodriguez's Fourth Amendment rights.

Back in March of 2018, the government obtained a search warrant (the "March 2018 warrant") of breathtaking scope that purported to allow it to seize virtually all digital devices at a residence in Anaheim, and then extract all content on each device from the entire lifespan of the device. While executing the search warrant, agents told Mr. Rodriguez that the warrant did not allow them to search his Jeep, which was parked in the garage. After he declined to give consent to search his car, they searched it anyway and seized two phones found inside. Then, rather than complying with the search warrant's 120-day deadline for retaining and searching those phones and the many other devices seized that day, the government let the deadline pass, and then waited *90 more days* before attempting to remedy its mistake by asking for a *nunc pro tunc* extension. This procedure has no basis in federal criminal law and does not rectify the government's failure to follow its own proposed deadlines and the law.

Child pornography was eventually found on the two phones seized from the Jeep, and a single image of child pornography was found on a third phone seized from inside the home, which together serves as the basis for the instant charges. Mr. Rodriguez now moves under the Fourth Amendment to suppress the evidence obtained from the seized digital devices on several grounds. *First*, the original March 2018 search warrant was invalid because it was lacking in probable cause, overbroad, and not particularized. *Second*, even assuming the original warrant was valid, the government repeatedly failed to comply with timing requirements set forth in the March 2018 warrant, as well as subsequent warrants, and unconstitutionally retained (and possibly searched) devices when it was not permitted to do so. The evidence obtained from these devices in violation of Mr. Rodriguez's Fourth Amendment rights must be suppressed.

II. BACKGROUND[1]

A. The Devices At Issue

The government seized 18 devices from Mr. Rodriguez's home on March 9, 2018. Child pornography was ultimately found on 3 of the 18 devices: 2 phones seized from inside the Jeep and 1 phone seized from inside the home. The remaining 15 devices were found to not contain any evidence and were returned. The three devices on which child pornography was found are listed in the following table:

Description	**Identifier**	**Seized From**
Black LG Android Cell Phone, Model Number LGLS991, IMEI Number 357355062960973 ("Black LG")	1B6	Bedroom
Silver Samsung cell phone with broken screen, Model Number SM-J327P ("Silver Samsung")	1B7	Jeep
Gold LG Cell Phone with broken screen, Model Number LS990, Serial Number 410KPVH0351583 ("Gold LG")	1B8	Jeep

B. The March 2018 Search Warrant

1. The government searched Mr. Rodriguez's residence and seized 18 digistal devices, most of which were later returned.

On March 5, 2018, the government obtained a search warrant for a residence in Anaheim. *See* Ex. 1. Around 6:00 a.m. on March 9, 2018, fifteen members of the Sexual Assault Felony Enforcement ("SAFE") team executed the search warrant at Mr. Rodriguez's home. While there, they interviewed Mr. Rodriguez, his mother, and his then-wife. During their interrogation of Mr. Rodriguez, two agents asked for his permission to search his Jeep that was parked in the garage. *See* Ex. 2 at 7:11:08-

[1] The declaration of Mr. Rodriguez (Exhibit 12), required under Local Criminal Rule 12-1.1, is provided pursuant to *Simmons v. United States*, 390 U.S. 377, 390-394 (1968), and Mr. Rodriguez does not waive his Fifth Amendment privilege.

7:11:36 a.m. Mr. Rodriguez asked: "Does the search warrant cover that?" The agents responded: "It doesn't include the vehicles." Mr. Rodriguez then clearly stated: "I'm not gonna give you consent to search." *Id.* Nevertheless, the government searched the Jeep and seized two cell phones found inside.

2. More than 90 days after the search warrant expired, the government sought a retroactive extension.

Pursuant to the March 2018 search warrant, the government had 120 days to retain and search the devices. Ex. 1 at USAO 525 ¶4.a. The 120 days came and went. Then another 90 days passed. On October 10, 2018—day 215—the government belatedly applied for what they called a "*nunc pro tunc*," i.e., retroactive, extension to the search warrant, citing a vague and unspecified "miscommunication" for its purported oversight. Ex. 3.

As discussed in detail below, the government indicated it needed additional time to complete "the review of the contents . . . as well as complete the search of the devices not yet searched." *Id.* at USAO 563 ¶8. As a result, the government asked for (1) a retroactive extension of 91 days for the government to retain the seized devices; and (2) an additional 60 days to complete its review of the devices. *Id.* at USAO 564 ¶¶13-14. The government cited no law or other authority in support of its novel request for a retroactive extension. The court approved the government's request the same day, making clear that the government had "up to and including December 9, 2018" to retain and search the six devices listed. *Id.* at USAO 568.

3. Following the first extension, the government obtained two more extensions.

For the second time, the government allowed its deadline to expire before requesting an extension. On December 10, 2018—one day after the prior extension had expired—the government filed an "Ex Parte Application for a Second Extension of Time Within Which to Retain and Search Digital Devices." Ex. 4. In its application, the government explained that it needed additional time to "complete its review" of the

digital devices. *Id.* at USAO 576 ¶10. As a result, it asked for yet another 90 days, until March 10, 2019, to retain and search the Black LG, the Silver Samsung, and the Gold LG phones. *Id.* at USAO 577 ¶11. The court granted the request the same day.

Though it had already been granted several prior extensions, on March 6, 2019, the government filed yet another "Ex Parte Application for a Third Extension of Time Within Which to Retain and Search Digital Devices." Ex. 5. In its application, the government requested an additional 90 days, to June 9, 2019, to "complete its review" of the three digital devices. *Id.* at USAO 586-87 ¶¶ 13-14. The government included as its purported justification the exact same language it had in its prior application: that forensic review of digital devices is "time consuming." *Compare* Ex. 5 at USAO 587 ¶13(d) *with* Ex. 4 at USAO 587 ¶13(d). The court granted the request the following day.

C. The April 2020 Search Warrant

1. The government obtained a new search warrant.

After seeking three extensions to the original March 2018 search warrant, the government sought an entirely new search warrant on April 21, 2020 (the "April 2020 warrant"). In the affidavit in support of the search warrant application, the affiant stated that the FBI had completed its review of 15 of the 18 devices seized on March 9, 2018 and sought the warrant "for additional time to search the remaining three" devices. Ex. 6 at USAO 506 ¶7. The declarant explained that he had taken over the case in March 2019, and due to his "heavy caseload," he was unable to complete his "review of the SUBJECT DEVICES and write the necessary forensic reports before expiration of the third extension." *Id.* at USAO 515 ¶24.

The April 2020 warrant contained the same 120-day deadline to search the devices and the same retention requirements as the March 2018 warrant. *Id.* at USAO 500 ¶2.c.

2. Over a month late, the government applied for an extension.

The 120-day deadline set forth in the April 2020 warrant expired on August 19, 2020. For the third time in this case, the government failed to file a timely request for an extension. More than a month after the deadline had passed, on September 30, 2020, the government finally requested an extension. Ex. 7. The declaration of counsel submitted in support of this request admitted that the 120-day deadline set forth in the April 2020 warrant "expired on August 19, 2020," but claimed that no additional searching occurred after that date. *Id.* at USAO 2857 ¶6. The declaration mentioned the original search warrant, but not the government's failure to follow its deadlines or its belated request for a retroactive extension. The government sought a 120-day extension to complete its review of the subject devices, and the court granted it. *Id.* at USAO 1043.

D. The October 2023 Search Warrant.

On October 13, 2023, the government again obtained an entirely new search warrant, the third warrant in this case. Ex. 8. Yet another new agent had been assigned to the case in October 2022. *Id.* at USAO 1195 ¶4. According to his declaration, he had learned in June 2023 that the final FBI forensic report of the subject devices had been burned to a DVD, but he "believe[d] that an error was made," which caused certain evidence to be saved "in a format that is not currently accessible." *Id.* at USAO 1196 ¶7. In order to recover the lost items, the affiant explained, "[a]n additional search is now required to re-bookmark and seize these items." *Id.* at USAO 1199 ¶9. The affiant attached the initial March 2018 search warrant, but did not relate the prior history, including the government's failure to comply with multiple earlier deadlines.

III. ARGUMENT

A. Legal Standard

The Fourth Amendment protects against "unreasonable searches and seizures." U.S. Const. amend. IV. It was adopted largely to prevent "general, exploratory rummaging in a person's belongings" and the attendant privacy violations. *Coolidge v.*

New Hampshire, 403 U.S. 443, 467 (1971). The government must have a warrant to search a cell phone. *See Riley v. California*, 573 U.S. 373 (2014).

Here, the government initially had a warrant to search Mr. Rodriguez's home and devices seized therefrom, but its conduct was nevertheless unconstitutional. *First*, the March 2018 search warrant was invalid on its face because it was based on stale evidence and failed to meet the Fourth Amendment's specificity requirements. *Second*, even assuming the warrant was valid, the government violated it, by allowing it to expire but continuing to retain (and possibly search) the seized devices for more than ninety days without authorization.

B. The March 2018 search warrant was based on stale evidence and not supported by probable cause.

"A warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky v. King*, 563 U.S. 452, 459 (2011); *see also United States v. Brobst*, 558 F.3d 982, 993 (9th Cir. 2009). Probable cause exists when, under the totality of the circumstances set forth in the affidavit in support of the warrant, "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

As the Supreme Court recognized over 90 years ago, the proof of probable cause "must be of facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause *at that time*." *Sgro v. United States*, 287 U.S. 206, 210 (1932) (emphasis added). "Information offered to support a search warrant application becomes stale when enough time has elapsed such that there is no longer sufficient basis to believe that the items to be seized are still on the premises." *United States v. Grant*, 682 F.3d 827, 835 (9th Cir. 2012) (internal quotation marks omitted); *see also Durham v. United States*, 403 F.2d 190, 193 (9th Cir. 1968).

The March 2018 search warrant was not supported by probable cause because it was based entirely on stale evidence. The purported basis for searching the apartment

at 3052 West Cheryllyn Lane was that on August 12, 2017, a user on the Kik messaging application with the profile name "talleyho14" had sent undercover officer Bernell Trapp a Dropbox link containing child pornography. Ex. 1 at USAO 539 ¶11. In the search warrant application, Agent Trapp stated under penalty of perjury that, according to information supplied by Kik on August 13, 2017:

> between June 29, 2017, and August 1, 2017, the Subject Account used IP address 172.90.36.99 (the "Suspect IP Address") on 19 different occasions, including on August 12, 2017, to log into "KIK" Account "talleyhol4."

Id. at USAO 540 ¶13. Agent Trapp further declared that, according to information provided by Charter Communications on August 14, 2017:

> the Subscriber Account using IP Address 172.90.36.99 on August 12, 2017, was assigned to "Maca Ortiz" at the SUBJECT PREMISES. Based on this information, I believe that when TALLEYHO shared the suspected child pornography with me on August 12, 2017, s/he did so from the SUBJECT PREMISES.

Id. at USAO 541 ¶14.

These paragraphs do not meet the probable cause requirement. To begin, Agent Trapp's description of the information provided by Kik is inaccurate. The first date reflected in the Kik returns when "talleyho14" was associated with the relevant IP address was *July 31, 2017*—nearly a month later than the June 29, 2017 date he provided. Ex. 9 at USAO 2818. This error matters. Rather than connecting to the IP address regularly over the course of six weeks, the user only connected to it during a two-week period. This makes it far less likely that evidence of the crime would be found at the apartment, especially given the dated nature of the evidence.

Even more importantly, the last connection to the IP address reflected in the Kik returns occurred on August 13, 2017—*almost seven months* before the government

applied for the original search warrant. *Id.* at USAO 2849. By the time the government requested its search warrant, this was stale information. The Ninth Circuit has found that similarly dated information invalidates a search warrant. *See*, *e.g.*, *Durham*, 403 F.2d at 193 (suppressing evidence obtained with search warrant based on 4-month old evidence related to counterfeit notes); *Grant*, 682 F.3d at 835 (9-month old evidence regarding a gun used in a homicide was stale and required suppression).

The staleness concerns are particularly acute here. *First*, the government did not have any information regarding who specifically at the residence was using the "talleyho14" account. They simply knew that someone with that account shared suspected child pornography on August 12, 2017 and had connected to the apartment's IP address the prior two weeks. This could have been a guest staying at the home for a limited time or a roommate who had moved out. It could have even have been someone who hacked into the WiFi network or someone in a nearby apartment who used the network without permission. The affidavit provides no reason to think it was someone who was living at the residence in the first place, let alone a resident still living there seven months later, in March 2018.

Second, the government's information that "all the Wi-Fi networks in range of the SUBJECT PREMISES were password protected" came many months later. Ex. 1 at USAO 541 ¶15. Agent Trapp's surveillance on the Wi-Fi networks was completed on or about February 13, 2018, six months after the suspected child pornography was shared. *Id.* The government presented no information to the Magistrate Judge suggesting that back in August 2017, the Wi-Fi networks were password protected. Thus, the individual who had shared child pornography could have been a neighbor, a long-term visitor of a nearby unit, or even a frequent passerby.

Finally, the Kik returns show that in addition to connecting to the Cheryllyn IP address, the "talleyho14" account was also associated with *25 other* IP addresses over the roughly two weeks for which Kik supplied information. Ex. 9. Indeed, on August 12, 2017, the day the suspected child pornography was shared, "talleyho14" used 5

other IP addresses. *Id.* at 2847-2849. The affidavit says nothing about this, or about the locations associated with the dozens of other IP addresses.

Because the March 2018 search warrant was based on stale information and thus lacked probable cause, all evidence obtained as a result of the warrant must be suppressed.

C. The March 2018 search warrant was overbroad and insufficiently particular.

Even if the Court finds the information in the March 2018 warrant application was not stale, the warrant failed to comply with the Fourth Amendment's specificity requirements. "To determine whether a warrant lacks sufficient specificity, we must examine both the warrant's particularity and its breadth." *United States v. Kow*, 58 F.3d 423, 426 (9th Cir. 1995). The particularity requirement "makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927).

In determining whether a warrant is sufficiently particular, courts consider the following factors: "(1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued." *United States v. Adjani*, 452 F.3d 1140, 1148 (9th Cir. 2006). The particularity requirement "is necessarily tied to the . . . probable cause requirement." *In re 650 Fifth Ave. & Related Props.*, 830 F.3d 66, 98 (2d Cir. 2016). Probable cause requires "a reasonable nexus between the crime or evidence and the location to be searched." *United States v. Crews*, 502 F.3d 1130, 1136-37 (9th Cir. 2007).

There are "heightened specificity concerns in the computer context, given the vast amount of data they can store." *Adjani*, 452 F.3d at 1149. A warrant that purports

to "authorize the seizure of, essentially, all documents" exceeds the scope of probable cause. *United States v. Wey*, 256 F. Supp. 3d 355, 393 (S.D.N.Y. 2017).

1. The March 2018 search warrant was not particularized and was overbroad.

The March 2018 warrant fails on each prong of the particularity analysis. When it applied for the search warrant, the government knew that someone with the username "talleyho14" had communicated on the Kik mobile messaging application between August 12, 2017 and August 15, 2017, and had shared suspected child pornography via a Dropbox link. Ex. 1 at USAO 539-540 ¶¶ 10-13. It also suspected that this unnamed individual was connected with the subject premises because "talleyho14" had used an IP address traced to the residence. *Id.* at USAO 540-541 ¶¶13-14. Thus, the government was aware of a specific timeline, two particular platforms, and a single username.

The search warrant, in contrast, allowed the seizure of "[a]ny digital device *capable of being used* to commit, further, or store evidence of" possession or distribution of child pornography—in other words, virtually any digital device on the premises. *Id.* at USAO 528 ¶5.a (emphasis added).[2] And once the government seized a digital device, it was permitted to "subject *all of the data*" within it to search protocols to determine whether it contained sought-after information. *Id.* at USAO 525, ¶4.b.i (emphasis added).

Moreover, despite the fact that the conduct purportedly providing probable cause was limited to three days in August 2017, the search procedures set forth in the warrant contain no time limitation whatsoever. *Id.* Thus, the warrant permitted the government to search an entire digital device, over its entire lifetime, simply because the device could theoretically be used to store or share child pornography. This is improper. *See*

[2] The breadth of this provision is illustrated by the wide variety of devices the agents seized (and later returned), which included an Xbox and multiple Nintendo devices,

United States v. Jolly, 2:20-cr-00438-MCS, ECF No. 248 (C.D. Cal.) (warrant overbroad because probable cause stemming from three specific arrests over a two-month period "does not provide probable cause to search every text on the Apple Watch"); *United States v. Roberts*, 430 F. Supp. 3d 693, 717 (D. Nev. 2019) (warrant impermissibly overbroad where it permitted search of phone extending four days before the burglaries mentioned in the warrant affidavit). When the government knows when the target offense occurred, "there is no justification for an unrestricted search without any temporal limitations." *United States v. Lofstead*, 574 F. Supp. 3d 831, 843 (D. Nev. 2021).

Beyond digital devices, the warrant also permitted the government to seize a wide swath of other records, including "[a]ny records, documents, programs, applications, or materials, including electronic mail and electronic messages" pertaining to:

- "peer-to-peer file sharing software"
- "accounts with any Internet Service Provider"
- "ownership and/or possession of the SUBJECT PREMISES"
- "ownership and/or possession and/or use of any digital device(s) found inside the SUBJECT PREMISES."

Ex. 1 at USAO 522 ¶¶f-i.

These categories are not tethered to the suspected child pornography which was the basis for the warrant. Under these provisions, the government could seize, for example, homeowners association bylaws, announcements, and policies, as well as work-related emails, chat messages, and applications for anyone in the residence. *Id.* ¶i. There is no basis, let alone probable cause, to support this. *See e.g., Wey*, 256 F.Supp.3d at 385 (warrant lacked particularity where it set forth "expansive categories of often generic items subject to seizure—several of a 'catch-all' variety—without, crucially, any linkage to the suspected criminal activity").

Thus, there was no probable cause for the government to seize the wide swath of items described in the warrant. And the government could have easily described the items sought with more particularity, given the specific information it had at the time. These two problems compound into a third problem with the search protocols. The purportedly objective standards guiding the agents' searches of the digital devices were premised on identifying "only the specific items to be seized under [the] warrant." Ex. 1 at USAO 525 ¶4.b. But because, as explained above, the list of "items to be seized" is itself overbroad, there is no objective standard by which to differentiate what falls within the scope of the warrant and what does not. These deficiencies are particularly concerning given that digital devices such as cell phones carry a "digital record of nearly every aspect of [American's] lives." *Riley*, 573 U.S. at 395.

The warrant's lack of particularity and overbreadth is illustrated by what was ultimately seized: of the 18 devices the government seized on March 9, 2018, the agents found child pornography on only 3 devices (one of which had only 1 image), and returned the remaining devices. *See United States v. Weber*, 923 F.2d 1338, 1344 (9th Cir. 1990) ("[S]earches with a substantial risk of failure are exactly those for which there is no probable cause in the first place.").

Because the March 2018 search warrant did not meet the Fourth Amendment's specificity requirements, all evidence seized pursuant to that warrant should be suppressed.

2. The search of the Jeep further illustrates the overbreadth of the warrant.

In their first interrogation of Mr. Rodriguez on March 9, 2018, agents told him the search warrant did not allow them to search his Jeep, and Mr. Rodriguez declined to give his consent to search the car.[3] Ex. 2 at 7:11:08-7:11:36 a.m. To the extent the

[3] The agents' statements are consistent with the fact that the government in this District and elsewhere routinely obtains search warrants that explicitly include vehicles within the "premises to be searched," in both child pornography and other cases, and could have done so here.

Court finds that, contrary to the agents' assertions, the government was permitted to search the Jeep pursuant to the search warrant, this further demonstrates the warrant's overbreadth.

The sole mention of vehicles in the entire search warrant application is the bare assertion that individuals with a sexual interest in children "usually maintain" their collections of child pornography in "a safe, secure, and private environment, such as their homes, vehicles, or nearby, so they can view the child pornography at their leisure." Ex. 1 at USAO 543 ¶17.c.

This type of generic statement does not come close to establishing probable cause, as the Ninth Circuit held in *Weber*, 923 F.2d at 1343-45, also a child pornography case. In an attempt to establish probable cause to search the defendant's home, the agent's affidavit recited general statements about the proclivities of "pedophiles and/or child pornography collectors." *Id.* at 1341. This included assertions that such individuals retain photographs for "many years," and that they sometimes conceal such materials in "safety deposit boxes, private commercial storage spaces, beneath homes, buried, in automobiles, hidden inside of legitimate books, at work places, etc." *Id.* The Ninth Circuit rejected these statements as insufficient "rambling boilerplate recitations." *Id.* at 1345. The court found there was "not a whit of evidence in the affidavit indicating that [the defendant] was a 'child molester'" or was otherwise in the category of pedophiles or collectors about which the agent opined. *Id.* at 1345, 1341. The Ninth Circuit held that the evidence seized pursuant to the warrant should be suppressed. *Id.* at 1346.

The reasoning of *Weber* applies with even more force here, for two reasons. *First*, unlike in *Weber*, the government was not specifically targeting Mr. Rodriguez when they executed the search warrant. He is not named anywhere in the search warrant application. Rather, the application simply alleges that *someone* had sent a link to child pornography from the target address. *See* Ex. 1 at USAO 532 ¶6 (stating that "an individual" sent a link to suspected child pornography); *id.* at USAO 539-40 ¶¶11-

13 (describing the individual only by their Kik username). The only specific person identified in the application was Maca Ortiz, the purported account holder of the relevant internet subscriber account. *Id*. at USAO 540 ¶¶ 14, 16.

Second, the materials at issue in *Weber* were found inside the defendant's home, whereas the agents in this case searched Mr. Rodriguez's vehicle parked in a detached garage on a different level of the building and hundreds of feet from the apartment's entrance. Vehicles, by their nature, require particular attention to probable cause. A car parked on a home's premises could belong to a resident, or it could belong to a visitor, someone who rents the parking space, a delivery person, a handyman, or someone else. Moreover, because a vehicle is inherently mobile and can come and go, there must be a particularized and timely justification for searching it. That was lacking here.

If the government's general assertion that people sometimes store child pornography in cars were sufficient to establish probable cause to search the Jeep, that same paragraph in the March 2018 search warrant would allow the government to search any "private environment" that happens to be "nearby" any individual associated with the address. *See* Ex. 1 at USAO 543 ¶17.c (asserting that individuals with a sexual interest in children maintain their collections "in a safe, secure, and private environment, such as their homes, vehicles, *or nearby*") (emphasis added). That is not the law. *Cf. Weber*, 923 F.2d at 1344 ("to find probable cause . . . would be to justify virtually any search of the home of a person who has once placed an order for child pornography"). Because there was no probable cause to search any vehicles impliedly encompassed within the warrant, this further establishes that the search warrant was overbroad.

In sum, the search warrant was invalid on its face for multiple reasons and all evidence obtained from the devices seized pursuant to that warrant must therefore be suppressed.[4]

D. Even if the March 2018 search warrant was valid, the government failed to follow its requirements, which independently requires suppression.

1. The government is required to comply with the terms of its search warrants, including any deadlines contained therein, and failure to do so requires suppression.

Rule 41(e)(2) of the Federal Rules of Criminal Procedure, which requires that a warrant generally must be executed within 14 days, does not set forth a "presumptive national or uniform time period" in which off-site copying or review of electronically stored information must take place. Fed. R. Crim. Proc. 41(e)(2), 2009 Advisory Comm. Notes. However, this "does not prevent a judge from imposing a deadline for the return of the storage media or access to the electronically stored information at the time the warrant is issued." *Id.*

Warrants issued in this District, including the warrants at issue in this case, routinely set forth specific deadlines by which the government must complete its searches of digital devices, as well as specific rules for the retention of such devices. When the government does not follow these protocols, it is not operating pursuant to a valid warrant and suppression is appropriate. *See United States v. Kopankov*, 672 F.Supp.3d 862, 866-68 (N.D. Cal. 2023) (suppressing evidence obtained from cell phone where government violated warrant protocols by creating "mirror" of device after time to do so had elapsed); *United States v. Brunette*, 76 F. Supp. 2d 30, 42 (D.

[4] In addition to the reasons set forth in Mr. Rodriguez's Motion to Suppress under the Fifth Amendment, concurrently filed herewith, his statements to law enforcement during the execution of the search warrant on March 9, 2018 should also be suppressed as the fruits of a search that was unconstitutional under the Fourth Amendment.

Me. 1999) (in child pornography case, suppressing evidence gathered from a computer that was searched 2 days late because government "failed to adhere to the requirements of the search warrant and subsequent order [granting a 30-day extension]"); *United States v. Metter*, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012) (government's 15-month delay in reviewing seized and imaged electronic evidence was an unreasonable seizure requiring suppression).

2. As the government has acknowledged, the March 2018 search warrant contained restrictions regarding when the government could retain and search the seized devices.

Pursuant to the March 2018 search warrant, the government was required to comply with the following requirement:

> The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

Ex. 1 at USAO 525 ¶4.a. In other words, the government was required to search the seized devices within 120 days or seek an extension from the Court.

The warrant also set forth the following procedures for retention and return of the devices:

> d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.
>
> e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government

> may make and retain copies of such data, and may access such data at any time.
>
> f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

Id. at USAO 526-527 ¶¶ 4d-f.

Pursuant to these provisions, if the government's search, completed within 120 days or pursuant to an extension granted by the Court, revealed that a device did not contain any evidence within the scope of the warrant, the government was required to return that device and destroy any copies of it. If, on the other hand, the government's search revealed that a device contained, or itself constituted, evidence within the scope of the warrant, the government was permitted to retain that device (subject to certain limitations) and copies of the relevant data.

Lastly, the warrant provided for one other scenario in which the government was permitted to retain a device:

> g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

Id. at USAO 000527 ¶4.g.

Thus, the March 2018 search warrant was clear that the government could only retain a device under two circumstances: (1) if it determined that the device contained or constituted evidence falling within the scope of the warrant; or (2) during the 120-day search period, the government sought an order authorizing retention, for example because the government had technical difficulties fully searching a device. The government did not comply with these requirements.

3. The government failed to comply with the 120-day deadline in the March 2018 search warrant, and then waited another 90 days to get a so-called retroactive extension.

The March 2018 search warrant was executed on March 9, 2018. Ex. 3 at USAO 562 ¶6. Thus, the government's 120-day deadline to retain and search the devices seized pursuant to that warrant expired on July 7, 2018. *Id*. On October 10, 2018—more than 90 days after the deadline expired and a full 215 days after executing the warrant—the government moved ex parte, under seal for relief.[5] Specifically, it filed a request it styled: "Government's *Ex Parte* Application for an Extension, *Nunc Pro Tunc*, of Time Within Which to Retain Digital Devices; And For an Extension of Time Within Which to Retain and Search Digital Devices," along with a declaration of counsel. Ex. 3.

In the declaration of counsel, the government acknowledged that the March 2018 search warrant "specifically authorized the seizure of digital devices from the SUBJECT PREMISES for a period of 120 days." Ex. 3 at USAO 562 ¶5. It also acknowledged that the deadline "to retain and search the SEIZED DIGITAL DEVICES" was July 7, 2018, more than three months before. *Id.* ¶6.

The government then summarized its investigation to date. It explained that on or about May 5, 2018, forensic specialists "began to prepare a forensic image" of the

[5] The defense was unaware of these developments until many years later, when Mr. Rodriguez was indicted and discovery was produced in this matter, and was therefore unable to object in real time.

two phones seized from the Jeep. *Id.* ¶7. Then, "[a]fter the forensic exams were completed" of those two phones (on some unspecified date), child pornography was discovered on the Gold LG cell phone. *Id.* The declaration stated that additional time was necessary to "complete the review of the contents . . . as well as complete the search of the devices not yet searched." *Id.* at USAO 563 ¶8; *id.* at USAO 565 ¶14.c (describing reports and images yet to be completed). Additionally, the declaration noted that agents had searched "all the thumb drives, the external SD memory cards, and the laptop" seized in March 2018, and found no responsive material. *Id.* at USAO 563 ¶9. Lastly, the declaration stated that agents had "no way to forensically search" the Nintendo devices, so no further efforts would be made as to those devices. *Id.* ¶10.

In sum, the government's ex parte application admits that (1) it had not completed its search of the devices pursuant by the 120-day deadline set forth in the March 2018 warrant; (2) it failed to seek an extension of the deadline before the warrant expired; (3) it nevertheless retained all of the seized devices more than 90 days after the deadline; and (4) it required a court order to retroactively permit its extended retention and any further searching. The sole justification the government provided for failing to comply with its own search warrant was an unspecified " miscommunication" between the agent and assigned prosecutor. *Id.* at USAO 564 ¶12. It provided no additional detail or explanation.

Even more troubling than the government's retention of the devices well past the deadline, the government appears to have been *searching* the devices during the time period when it had no valid warrant.[6] The government claimed in its request for an extension that it "halted its review of the SEIZED DIGITAL DEVICES, including the SUBJECT DIGITAL DEVICES, on July 7, 2018." *Id.* at USAO 564-65, ¶11. But that assertion is inconsistent with chain of custody records produced in this matter. For

[6] Mr. Rodriguez specifically requests an evidentiary hearing to explore to what extent the government searched the phones after the search warrant expired.

example, the FBI's chain of custody form for the Black LG phone (1B6) contains the following entry:

Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature:	8/16/18	Signature:	8/16/18
Printed Name/Agency: BERNELL TRAPP	10:45am	Printed Name/Agency: AMY WHITMAN/FBI	10:45am
Reason: TO CASE AGENT		Reason: REVIEW	

Ex. 10. On August 16, 2018—more than a month after the search warrant expired and months before the government sought a retroactive extension—Agent Trapp returned the Black LG phone to Agent Whitman for "Review." *Id.*[7] This suggests the government's representation in the search warrant application that it halted its review on July 7, 2018 was not accurate. It also appears to show the government was not only retaining, but may have been *searching*, the devices without a warrant. This violated the Fourth Amendment.

As for the government's attempt to fix its unconstitutional actions via a retroactive extension, it fails. *First*, the government did not file it "prior to the end of the search period," as required by the warrant. Ex. 2 at USAO 527 ¶4.g. And because the government was not permitted to continue its seizure of the devices after the 120-day deadline expired, its continued retention of the devices during that period constituted a prolonged, unconstitutional seizure. *See Brewster v. Beck*, 859 F.3d 1194, 1196 (9th Cir. 2017) ("'[A] seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests.'") (quoting *United States v. Jacobsen*, 466 U.S. 109, 124 & n.25 (1984)); *see also Sandoval v. Cnty. of Sonoma*, 72 F. Supp. 3d 997, 1004 (N.D. Cal. 2014), *aff'd*, 912 F.3d 509 (9th Cir. 2018) ("The Fourth Amendment protects an individual's interest

[7] The chain of custody log for the black Alcatel phone the government seized (1B17) has an identical entry on August 16, 2018, raising further questions regarding the government's activities during this time. Ex. 11.

in possessing his property, and that interest is implicated by a delay in returning the property, whether the property was seized for a criminal investigation, to protect the public, or to punish the individual."); *cf. United States v. Williams*, CR 13-302-PSG, Dkt. 156 (C.D. Cal. May 9, 2014) (granting motion to suppress where government waited 97 days to obtain a warrant after seizing digital devices due to an "oversight" because the agent was working on two simultaneous forensic reviews).

Second, there is no *nunc pro tunc* procedure to extend search warrants in the Federal Rules of Criminal Procedure. To the contrary, the rules governing search warrants make clear the importance of complying with specific timing requirements. *See, e.g.*, Fed. R. Crim. Proc. 41(e)(2)(A)(i) (warrant generally must be executed within 14 days); *id.* (f)(2)(B) (tracking-device warrant return due within 10 days after use has ended). Nor is the undersigned aware of any federal statute or other authority that provides for retroactive search warrant extensions.

To the extent courts may exercise *nunc pro tunc* authority at all, it is limited to correcting non-substantive "errors in the record." *United States v. Sumner*, 226 F.3d 1005, 1009–10 (9th Cir. 2000) (citing *Martin v. Henley,* 452 F.2d 295, 299 (9th Cir.1971)). "It does not imply the ability to alter the substance of that which actually transpired or to backdate events to serve some other purpose. . . . Rather, its use is limited to making the record reflect what the district court actually intended to do at an earlier date, but which it did not sufficiently express or did not accomplish due to some error or inadvertence." *Id.* (cleaned up); *see also Singh v. Mukasey*, 533 F.3d 1103, 1110 (9th Cir. 2008) (rejecting immigration petitioner's attempt to use *tunc pro tunc* procedure because there was no "clerical mistake or error of law").

As these authorities make clear, a *nunc pro tunc* extension was not proper here. The error at issue was the government's, not the court's. Moreover, the retroactive extension did not accomplish something the court intended to do at an earlier date. Rather, it was directly contrary to the 120-day deadline the court imposed in the initial search warrant. And the *nunc pro tunc* extension was not clerical but instead attempted

to "alter the substance of that which actually transpired," namely that the government had violated the Fourth Amendment by retaining (and possibly searching) devices after the deadline. *Sumner*, 226 F.3d at 1010.

Given that there is no legal basis to seek a *nunc pro tunc* extension to a search warrant, it is no surprise that the government's ex parte application did not contain a single legal citation to support its extraordinary request. The government then built on that extension to obtain two more extensions and two additional search warrants, spanning more than 5 years in all. *See* Parts II.B.3, II.C, and II.D above. Every subsequent extension and warrant, and the searches conducted based on them, were fruits of the original warrant and the government's unconstitutional actions. As a result, all evidence obtained pursuant to the government's *nunc pro tunc* extension, and the extensions and warrants that followed, should be suppressed. *See Wong Sun v. United States*, 371 U.S. 471, 488 (1963).

IV. CONCLUSION

For the foregoing reasons, Mr. Rodriguez respectfully requests that this Court grant his motion to suppress and suppress all evidence obtained pursuant to the March 2018 search warrant.

Respectfully submitted.

CUAUHTEMOC ORTEGA
Federal Public Defender

DATED: June 24, 2024

By */s/ Terra Castillo Laughton*
TERRA CASTILLO LAUGHTON
Deputy Federal Public Defender

INDEX OF EXHIBITS

Ex. 1	March 5, 2018 Search Warrant (USAO 519)
Ex. 2	Recorded Interrogation of Mr. Rodriguez (First Interrogation, Part 1)
Ex. 3	Government's Ex Parte Application for an Extension, Nunc Pro Tunc, of Time Within Which to Retain and Search Digital Devices (USAO 558)
Ex. 4	Government's Ex Parte Application for a Second Extension of Time Within Which to Retain and Search Digital Devices (USAO 571)
Ex. 5	Government's Ex Parte Application for a Third Extension of Time Within Which to Retain and Search Digital Devices (USAO 581)
Ex. 6	April 21, 2020 Search Warrant (USAO 494)
Ex. 7	Government's Ex Parte Application for Extension of Time to Retain and Search Digital Devices (USAO 2854) & Order (USAO 1042)
Ex. 8	October 13, 2023 Search Warrant (USAO 1183)
Ex. 9	Kik Emergency Disclosure Request Response (USAO 2817)
Ex. 10	FBI Evidence Chain of Custody for 1B6 (USAO 2862)
Ex. 11	FBI Evidence Chain of Custody for 1B17 (USAO 1017)
Ex. 12	Declaration of Rene Rodriguez

CUAUHTEMOC ORTEGA (Bar No. 257443)
Federal Public Defender
TERRA D. CASTILLO LAUGHTON (Bar No. 321683)
(E-Mail: Terra_Laughton@fd.org)
Deputy Federal Public Defender
411 W. Fourth St., Suite 7110
Santa Ana, California 92701
Telephone: (714) 338-4500
Facsimile: (714) 338-4520

Attorneys for Defendant
RENE RODRIGUEZ

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

RENE RODRIGUEZ.

Defendant.

Case No. 8:23-cr-00123-DOC

DECLARATION OF TERRA CASTILLO LAUGHTON IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS EVIDENCE OBTAINED IN VIOLATION OF THE FOURTH AMENDMENT

DECLARATION OF TERRA CASTILLO LAUGHTON

I, Terra D. Castillo Laughton, hereby state and declare as follows:

1. I am an attorney with the Office of the Federal Public Defender for the Central District of California. I am licensed to practice law in the State of California and I am admitted to practice in this Court. I have been appointed to represent Defendant Rene Rodriguez in the above-captioned case.

2. Filed concurrently with this declaration as **Exhibit 1** is a true and correct copy of the March 5, 2018 search warrant ("March 2018 search warrant"), produced in discovery in this case beginning at USAO_519.

3. Lodged concurrently with this declaration as **Exhibit 2** is a true and correct copy of a video produced by the government in discovery in this case as USAO_004.

4. Filed concurrently with this declaration as **Exhibit 3** is a true and correct copy of the government's application for a *nunc pro tunc* extension to the March 2018 search warrant, produced by the government in discovery in this case beginning at USAO_558.

5. Filed concurrently with this declaration as **Exhibit 4** is a true and correct copy of the government's application for second extension to the March 2018 search warrant, produced by the government in discovery in this case beginning at USAO_571.

6. Filed concurrently with this declaration as **Exhibit 5** is a true and correct copy of the government's application for third extension to the March 2018 search warrant, produced by the government in discovery in this case beginning at USAO_581.

7. Filed concurrently with this declaration as **Exhibit 6** is a true and correct copy of the April 21, 2020 search warrant ("April 2020 search warrant"), produced in discovery in this case beginning at USAO_494.

8. Filed concurrently with this declaration as **Exhibit 7** is a true and correct

copy of the government's application for an extension to the April 2020 search warrant, produced by the government in discovery in this case beginning at USAO_2854, along with the order granting that request, which was produced by the government in discovery in this case beginning at USAO_1042.

9. Filed concurrently with this declaration as **Exhibit 8** is a true and correct copy of the October 13, 2023 search warrant, produced in discovery in this case beginning at USAO_1183.

10. Filed concurrently with this declaration as **Exhibit 9** is a true and correct copy of Kik's Emergency Disclosure Request Response dated August 13, 2017, produced in discovery in this case beginning at USAO_2817.

11. Filed concurrently with this declaration as **Exhibit 10** is a true and correct copy of an evidence chain of custody log produced by the government in discovery in this case as USAO_2862.

12. Filed concurrently with this declaration as **Exhibit 11** is a true and correct copy of an evidence chain of custody log produced by the government in discovery in this case as USAO_1017.

13. Filed concurrently with this declaration as **Exhibit 12** is a true and correct copy of Mr. Rodriguez's signed declaration in support of his Motion to Suppress under the Fourth Amendment. This declaration, required under Local Criminal Rule 12-1.1, is provided pursuant to *Simmons v. United States*, 390 U.S. 377, 390-394 (1968), and Mr. Rodriguez does not waive his Fifth Amendment privilege.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge. Executed on June 24, 2024 at Santa Ana, California.

Terra Castillo Laughton

TERRA D. CASTILLO LAUGHTON